EDB Masterclass

A Knowledge Session on Ensuring "Secure" Digital Transformation

EDB

PostgreSQL

Everything can be hacked!

Mr. Saket Modi

Saket Modi is the Co-founder and CEO of Safe Security, a Cybersecurity and Digital Business Risk Quantification platform company. A computer science engineer by education, he founded Safe Security in 2012 while in his final year of engineering.

Safe Security protects the digital infrastructure of multiple Fortune 500 companies around the world. Saket is a part of Fortune Magazine's 40-under-40, Entrepreneur Magazine's 35-under-35, Forbes Magazine's 30-under-30 lists, among others.

Security considerations in app development

Mr. Dave Page

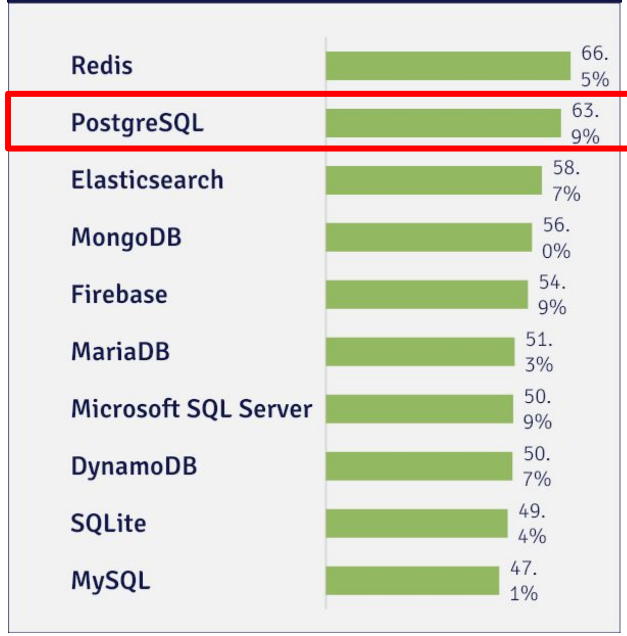
Dave Page is VP and Chief Architect, Database Infrastructure, currently working in the CTO team on research and development, best practices with Postgres, and providing high-level guidance and support for key customers.

Dave has been working with PostgreSQL since 1998 and is one of seven members of the open source project's Core Team, as well as serving as Secretary of the Board of PostgreSQL Europe and Chairman of the PostgreSQL Community Association of Canada.

Why PostgreSQL?

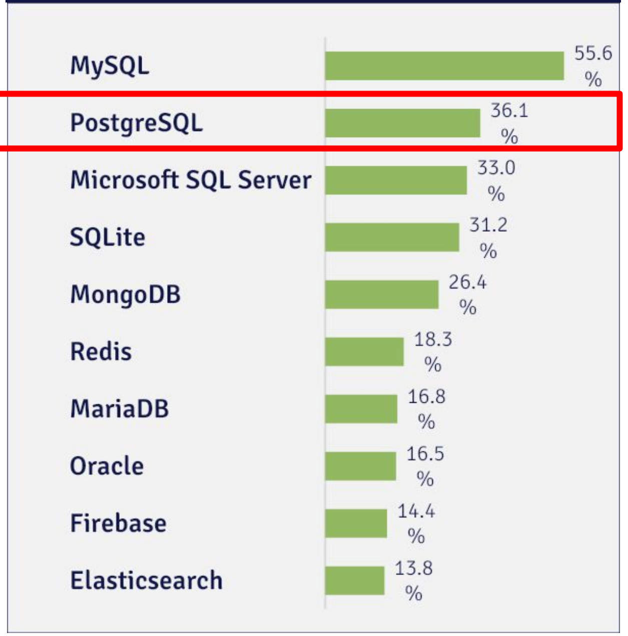
PostgreSQL won

Most **popular** database



and

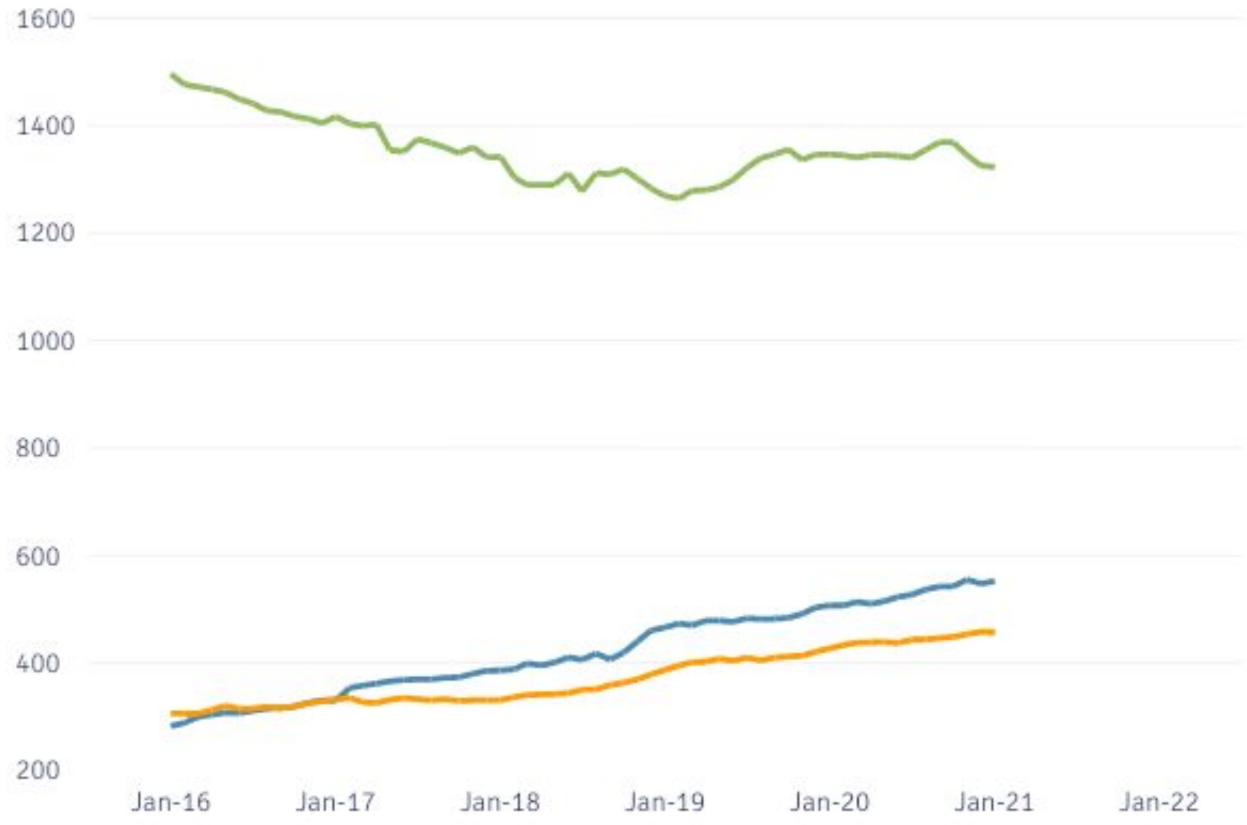
Most **loved** database



Source: Stack Overflow Developer Survey, 2020

It's the only database that people use and love...

PostgreSQL is winning



Oracle popularity

PostgreSQL popularity

MongoDB popularity

Source: DB-Engines.com, 2021

DBMS of the YEAR 2020
PostgreSQL
DB-Engines.com
DBMS of the YEAR 2018
DBMS of the YEAR 2017

Year after year

Why did PostgreSQL win?

It does everything...

- Migration
- New App Development
- Replatforming to Cloud and Containers
- System of Record
- System of Analysis
- System of Engagement

It works everywhere...

- Public Cloud - IaaS
- Public Cloud - DBaaS
- Private Cloud
- Virtual Machines
- Containers

and doesn’t lock you in

Why EDB?

We’re battle tested

Boundary pushing customers supported by world-class technologists

Over 300
dedicated PostgreSQL technologists

91%
customer satisfaction rating

Gartner FORRESTER

Recognized by leading analyst firms

ABN·AMRO Telefónica mastercard TOMTOM HYUNDAI GAP Alibaba.com edmunds.com Accertify Santander AT&T ERICSSON SONY

We’re a trusted partner

↗ Increase Speed to Market

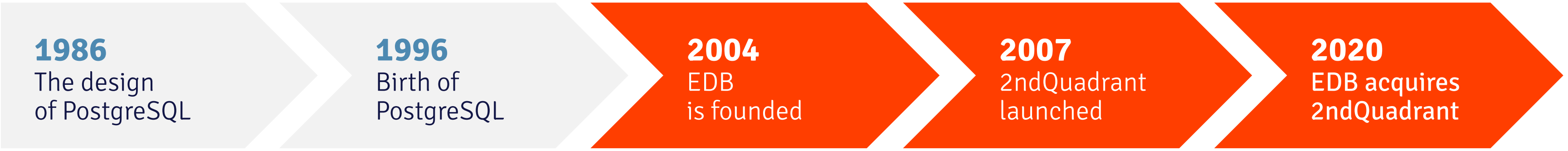
- Time to value
- Faster decisions
- Better products, faster
- Meet business needs

↘ Decrease Database Risk

- Performance and scalability
- Security and confidence
- 24x7 support
- Enterprise tooling

You don’t have to choose between going faster and going further

We're the PostgreSQL experts



1986
The design
of PostgreSQL

1996
Birth of
PostgreSQL

2004
EDB
is founded

2007
2ndQuadrant
launched

2020
EDB acquires
2ndQuadrant

Key PostgreSQL Contributions

EDB

- Heap Only Tuples (HOT)
- Materialized Views
- Parallel Query
- JIT Compilation
- Serializable Parallel Query

2ndQuadrant

- Hot Standby
- Logical Replication
- Transaction Control in Procedures
- Generated Columns

No company has contributed more to PostgreSQL

We have the most PostgreSQL experts

EDB TEAM INCLUDES:

- 300+ PostgreSQL technologists
- 26 PostgreSQL community contributors and committers
- Including founders and leaders like

Michael Stonebraker
"Father of Postgres" and EDB Advisor

Bruce Momjian
Co-founder, PostgreSQL Development Corp and PostgreSQL Core Team

Peter Eisentraut
PostgreSQL Core Team member

Robert Haas
PostgreSQL Major Contributor and Committer

Simon Riggs
PostgreSQL Major Contributor, Founder of 2ndQuadrant

Our portfolio delivers the PostgreSQL you need

Open, flexible, and enterprise-grade

Databases

PostgreSQL and extensions
for enterprise workloads

Tools

Monitoring, management,
scalability, high availability

Deployments

On-prem to the cloud
VMs to k8s to managed service

Expertise

24/7 technical support, remote
DBAs, professional services

Plans for every step of your journey

From dev/test to tier-1

	Community 360	Standard	Enterprise
	For organization who need PostgreSQL expertise and support	For businesses that have an open source strategy and need 24/7 support and additional tooling	For applications that require Oracle compatibility, enhanced security, and/or other enterprise features
EDB Postgres Advanced Enterprise-ready, Oracle-compatible PostgreSQL database			✓
PostgreSQL Open source database supported by EDB		✓	✓
EDB Tools Management, Backup, Failover, Migration, and Replication		✓	✓
Open source Tools	✓	✓	✓
Technical Support 24x7 expert technical support	✓	✓	✓
BDR The most advanced replication solution available for PostgreSQL		Optional	Optional

EDB™

BigAnimal: Faster, safer, smarter, better

Postgres Expertise

Expertise beyond the generalist cloud provider; we help steer the database roadmap and patch its bugs

Oracle Compatibility

Leave Oracle and further your cloud journey with a fully managed Postgres service

Continuous availability

High availability of your PostgreSQL clusters so you're always on, always available

Curious? Request a free trial today!
https://resources.biganimal.com/cloud-postgresql-trial

EDB portfolio

Delivering our customers the PostgreSQL they need

Your use cases

- New applications
- Database migrations
- Replatform to the cloud

Your requirements

- Availability
- Scalability
- Flexibility
- Expertise

The database you need

- PostgreSQL
- EDB Postgres Advanced
- EDB Postgres Extended

Where you want it

- On-premises | hybrid cloud | multi cloud
- Virtual machines
- Kubernetes

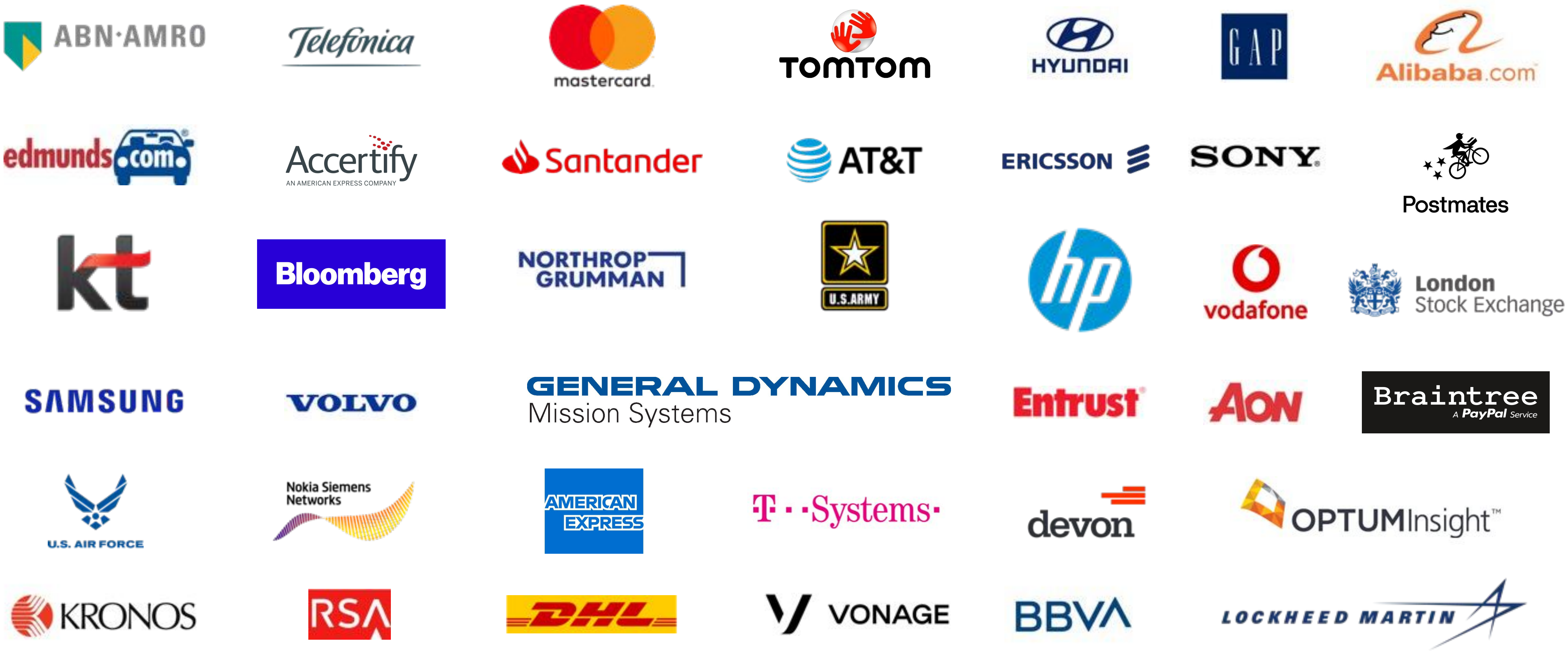
The tools you need

- EDB tools
- Open source tools

The help you need

- Expert 24/7 technical support
- Remote DBAs | Cloud DBAs
- Technical Account Managers
- Professional Services

Market success



Data Security Overview

Dave Page

2 February 2022

EDB

Dave Page

- EDB (CTO Office)
  - VP & Chief Architect, Database Infrastructure

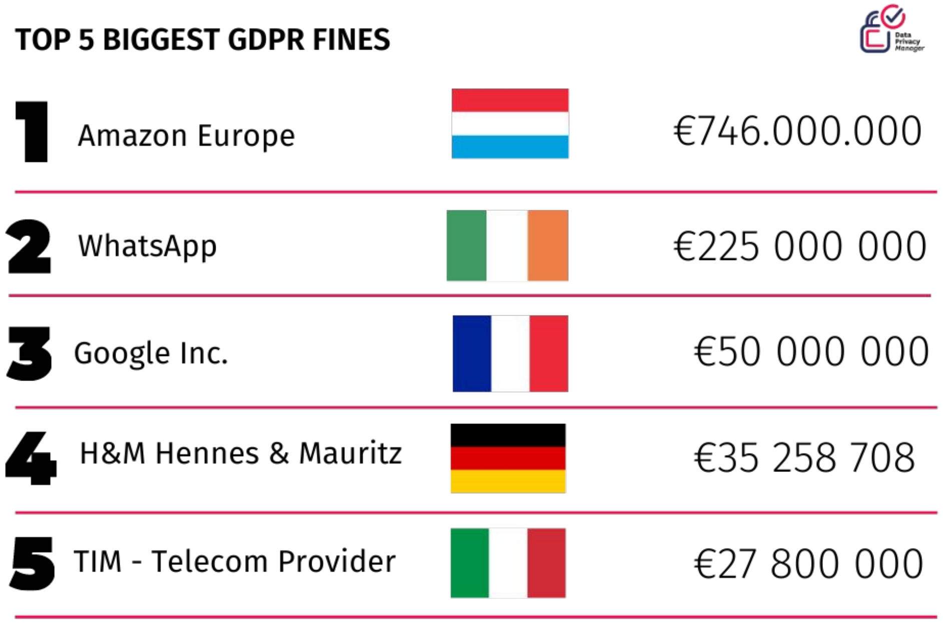
- PostgreSQL
  - Core Team
  - pgAdmin Lead Developer

Why?

- Business confidentiality:
  - Seems obvious!
  - We don't want to lose the competitive advantage

- Legal obligations:
  - Europe: GDPR
  - USA: HIPAA, FCRA, FERPA, COPPA, ...
  - India: PDP Bill 2019 (proposed)
  - Payment processing: PCI
  - ...

- Moral obligations:
  - Protect our employees privacy
  - Protect our customers privacy



TOP 5 BIGGEST GDPR FINES

1	Amazon Europe	€746.000.000
2	WhatsApp	€225 000 000
3	Google Inc.	€50 000 000
4	H&M Hennes & Mauritz	€35 258 708
5	TIM - Telecom Provider	€27 800 000

Fines can be huge if we get it wrong!

https://dataprivacymanager.net/5-biggest-gdpr-fines-so-far-2020/

How?

- Authentication
- Authorisation
- Accounting

Authentication

Ensure data consumers are who we think they are

- Protect the server:
  - VPN to ensure only expected users can access the network
  - Firewall to allow connections only from expected hosts
  - pg_hba.conf:
    - Limits access for specific users on specific hosts to specific databases
    - Defines the authentication requirements for connections (Kerberos, SCRAM etc)
  - *Could also be considered part of Authorisation*

- Be sure of users' identities, regardless of where they're connecting from:
  - Strong passwords
  - Multi-factor authentication
  - Consider use of Kerberos or Active Directory to ease management and enforce policies globally

- No shared user accounts or credentials!

Authorisation

Ensure users have the minimum access required

- Principle of Least Privilege:
  - Only allow users to access what they need to do their jobs
- Make use of roles and role membership for ease of management
- Grant permissions to "group" roles to enable specific tasks:
  - Databases: CONNECT, CREATE
  - Tables/views: SELECT, INSERT, UPDATE, DELETE
  - Functions/procedures: EXECUTE
  - Schemas: CREATE, USAGE
  - ...
- Row level security:
  - Restrict access to subsets of data, e.g. patient information may be restricted to a particular medical team
- Data masking/redaction:
  - Mask unnecessary information, e.g. show only the last 4 digits of a customer's credit card number

Accounting

Audit logging and alerting for everything of any possible importance

- Helps detect breaches soon as they happen to enable timely reporting to authorities before others make third party reports

- Can be critical when investigating network intrusion attempts

- Provides an audit trail for data access and changes:
  - Helps deter authorised but inappropriate data access (e.g. a staff member looking at a relatives personal information)
  - Can be useful when reverting unauthorised data changes

- Can help find culprits and plug security holes:
  - Who hacked the system?
  - How did they get in?
  - What improvements can we make?

Summary

- Make use of the AAA model
- Security is like an onion, with AAA applied throughout!
- This presentation only touches some of the basics
- There are far, far more topics that may be appropriate to study to meet your security requirements:
    - Application security
    - Virtual Private Clouds
    - 802.1q VLANs
    - SELinux
    - At-rest encryption
    - In-transit encryption
    - Physical security
    - PostgreSQL security definer functions
    - PostgreSQL security barrier views
    - …
    - …

Questions and resources

Questions?

- Best Practices in Security for PostgreSQL (webinar):
    - https://info.enterprisedb.com/Webinar_BestPracticesinSecurityforPostgreSQL.html

- How to Secure PostgreSQL: Security Hardening Best Practices & Tips (mega-blog):
    - https://www.enterprisedb.com/blog/how-to-secure-postgresql-security-hardening-best-practices-checklist-tips-encryption-authentication-vulnerabilities

- EDB Labs: Direct knowledge from EDB's technologists about PostgreSQL, the Postgres ecosystem, and open source
    - https://www.enterprisedb.com/edb-labs

Thank you!

edbpostgres.com

EDB™